Certificate of Filing by EFS-Web	
I hereby certify that this correspondence is being transmitted to the Patent and Trademark Office via EFS-Web at local date of:	
DATE: Mar. 16, 2007	S-SIGNATURE: /Robert H. Frantz/ Robert H. Frantz, Reg. No. 42,553

In the United States Patent and Trademark Office

In re the Application of:

Anthony Scott Moran	)	
Serial Number: 09/903,704	)	Group: 2131
Docket Number: AUS920010409US1	)	Examiner: Kaveh Abrishamkar
Filed on: 07/12/2001	)	
For: "Grouped Access Control List Actions"	)	

APPEAL BRIEF

Real Party in Interest per 37 CFR §41.37(c)(1)(i)

The subject patent application is owned by International Business Machines Corporation of Armonk, NY.

Related Appeals and Interferences per 37 CFR §41.37(c)(1)(ii)

None.

Status of Claims per 37 CFR §41.37(c)(1)(iii)

Claims 1 - 24 are finally rejected. Appellants request relief from the erroneous rejections of all pending claims.

Status of Amendments after Final Rejections per 37 CFR §41.37(c)(1)(iv)

No amendments to the claims have been submitted or entered after final rejections.

Summary of the Claimed Subject Matter per 37 CFR §41.37(c)(1)(v)

Appellants' invention solves a problem in the art relating to permission lists for controlling access to computer resources, such as computer disks, folders of files, databases, etc. Permission indicators are often single-character constants. Present technology at the time of filing Appellants' patent application used permission indicators which were static or pre-determined in their meanings. For example, the letter "k" would always mean permission by a user to "read" a file, regardless of which user was given the permission, and regardless of which file was being accessed. As such, with permission indicators having static meanings, only a finite set of meanings and permissions were possible due to the finite number of characters and numbers in the alphabet.

Appellants' invention solves this problem by providing permission lists in which the permission lists are made up of "permission indicators" contained within "permission containers", without increasing the size of the permission indicator (e.g. they are kept to just a single character). According to the invention, each indicator is "reusable" in that its meaning is relative to the permission container in which it resides. For example, the indicator "k" might mean permission to "read" a file in a first container, but might mean permission to "delete" a file in another container. This allows for an unlimited number of permission controls, limited only by the number of distinct characters in the alphabet multiplied by the number of different containers allowed in a system, all while maintaining single-character permission indicator sizes.

More specifically, independent Claim 1 sets forth a method of the invention for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, through the steps of:

(a) providing in a computer readable medium (para. 0024) an access control policy (paras. 0035, 0074; Fig. 8 #80) associated with said requested protected system resource (para. 0037) containing a permission list (para. 0070) of permitted identities and at least one action group tag with associated action indicators (paras. 0070, 0071);

(b) reusing (para. 0070) a finite quantity of action indicators among a plurality of action group tags to control a number of unique permissions less than or equal to the product (para. 0072) of the quantity of allowable action indicators and a

quantity of allowable action group tags (paras. 0071, 0072);

(c) evaluating (paras. 0082 - 0088; Fig. 9 #91 - 95, #97) said permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between permissible actions and members of a set of action indicators ; and

(d) granting (paras. 0082 - 0088; Fig. 9 #96, #98, #99) to a requesting computer or program authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

Claim 4 sets forth a method for managing permission indicators for computer system protected objects comprising the steps of:

(a) providing in a computer readable medium (para. 0024) a plurality of permission indicator containers (para. 0072) in an access control list (paras. 0035, 0070, 0074; Fig. 8 #80);

(b) associating a first set of permission indicators with a primary permission indicator container (paras. 0070 - 0072); and

(c) associating in a computer readable medium accessible by an authorization control system one or more additional sets of permission indicators with additional permission indicator containers, wherein said permission indicators are reused among said containers such that permission indicators may be categorized and grouped logically to control a number of unique permissions less than or equal to the product (para. 0072) of a quantity of allowable action indicators and a quantity of allowable action group tags (paras. 0082 - 0088; Fig. 9 #96, #98, #99).

Similarly, independent Claim 9 sets forth a computer readable medium encoded with software for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, the software performing the steps of:

(a) providing in a computer readable medium (para. 0024) an access control policy (paras. 0035, 0074; Fig. 8 #80) associated with said requested protected system

resource (para. 0037) containing a permission list (para. 0070) of permitted identities and at least one action group tag with associated action indicators (paras. 0070, 0071);

(b) reusing (para. 0070) a finite quantity of action indicators among a plurality of action group tags to control a number of unique permissions less than or equal to the product (para. 0072) of the quantity of allowable action indicators and a quantity of allowable action group tags (paras. 0071, 0072);

(c) evaluating (paras. 0082 - 0088; Fig. 9 #91 - 95, #97) said permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between permissible actions and members of a set of action indicators ; and

(d) granting (paras. 0082 - 0088; Fig. 9 #96, #98, #99) to a requesting computer or program authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

Accordingly, Claim 12 sets forth a computer readable medium encoded with software for managing permission indicators for computer system protected objects, wherein the software performs steps comprising:

(a) providing in a computer readable medium (para. 0024) a plurality of permission indicator containers (para. 0072) in an access control list (paras. 0035, 0070, 0074; Fig. 8 #80);

(b) associating a first set of permission indicators with a primary permission indicator container (paras. 0070 - 0072); and

(c) associating in a computer readable medium accessible by an authorization control system one or more additional sets of permission indicators with additional permission indicator containers, wherein said permission indicators are reused among said containers such that permission indicators may be categorized and grouped logically to control a number of unique permissions less than or equal to the product (para. 0072) of a quantity of allowable action indicators and a quantity of allowable action group tags (paras. 0082 - 0088; Fig. 9 #96, #98, #99).

Claim 17, however, is directed towards an authorization system for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, where the system includes:

(a) an access control policy disposed in a computer readable medium associated with said requested protected system resource, having a permission list of permitted identities and at least one action group tag with associated action indicators, wherein a finite quantity of action indicators are reused among a plurality of action group tags to control a number of unique permissions less than or equal to the product of the quantity of allowable action indicators and a quantity of allowable action group tags (paras. 0024, 0035, 0070 - 0074, Fig. 8 #80);

(b) a permission list evaluator for evaluating an access control policy permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between members of a set of action indicators (paras. 0082 - 0088; Fig. 9 #91 - 95, #97); and

(c) an authorization grantor adapted to grant authorization to a requesting computer or program to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag (paras. 0082 - 0088; Fig. 9 #96, #98, #99).

And, independent Claim 20 sets forth a system for managing permission indicators for computer system protected objects comprising:

(a) a plurality of permission indicator containers (para. 0072) for an access control list (paras. 0035, 0074; Fig. 8 #80) , said access control list being disposed in a computer readable medium (para. 0024);

(b) a first set of permission indicators associated with a primary permission indicator container (paras. 0037, 0070 - 0071); and

(c) one or more additional sets of permission indicators associated in said computer readable medium with additional permission indicator containers, wherein said permission indicators are reused (para. 0070 - 0072) among said containers such that permission indicators are categorized and grouped logically to control a

number of unique permissions less than or equal to the product (para. 0072) of a quantity of allowable action indicators and a quantity of allowable action group tags (paras. 0082 - 0088; Fig. 9).

Grounds for Rejection For Which Review is Sought per 37 CFR §41.37(c)(1)(vi)

Review by the Board of the rejections of Claims 1 - 24 under 35 U.S.C. §102(e) as being anticipated by published U.S. patent application 2001/0056494 A1 to Trabelsi (hereinafter "Trabelsi") is requested.

Arguments per 37 CFR §41.37(c)(1)(vii)

Rejections of Claims 1 - 24 under 35 U.S.C. §102(e) over Trabelsi

Improper Rejection of Previously Allowed Claims. In the first Office Action, dated December 16, 2004, Claims 3, 18 and 19 were indicated as being allowable by examiner Ramya Ananthanarayanan. In response to this indication, Appellants amended the steps, elements or limitations of Claim 3 into the independent claims of the application, and amended claim 3 to cover a different aspect of the invention. Surprisingly, after examiner Kaveh Abrishamkar took up the examination of the application, the allowability of Claim 3 (and correspondingly amended independent claims) was withdrawn without explanation.

In subsequent responses to the Examiner, Appellants objected to this change in position upon the reasons that the issuance of new rejections over newly cited art under 35 U.S.C. §102, therefore, may constitute improperly taking an entirely new approach, improperly attempting to reorient the point of view of a previous examiner, and/or improperly making a new search in the mere hope of finding something. *Amgen, Inv. V. Hoechst Marion Roussel, Inc.,* 126 F. Supp. 2d 69, 139, 57 USPQ2d 1449, 1499 - 50 (D. Mass. 2001), as cited in MPEP 706.04.

Examiner Ananthanarayanan's previous statements are of merit and weight, whereas the technical and legal expertise of all examiner's is certified by the Commissioner for Patents. Subsequent examiners of a patent application cannot simply set aside or discard positions and opinions by previous examiners of the same application. If this were permitted, then the legal and technical credibility of all patent examiners would be unfairly called into question, and applicants could be subjected to an unlimited number of shifts in position by examiners as the application is transferred from one examiner to another resulting in a gross violation of the precept of compact examination.

This is not just a matter of policy within the Office. It is a matter of improper denial of patent rights to the Appellants whereas at least one technical and legal expert is on the record in

the history of this prosecution in favor of patentability. This expert, the previous examiner, is of particular weight in the examination, being a trained employee of the USPTO.

Therefore, there is a first issue for review by the Board regarding the statement of record by the first examiner, Examiner Ananthanarayanan, agreeing with Appellants that the claims as earlier amended are allowable.

Whereas the current examiner, Examiner Abrishamkar, has failed to place any explanation or statements in the record regarding why the earlier holding of allowability was incorrect, despite repeated requests by the Appellants for explanation, then the claims should be allowed without the need for further examination because Appellants' first amendment simply complied with the allowability statement, and should have caused no need for additional searching or examination.

For this reason, Appellants submit that the current rejections are erroneous, and allowance of claims 1 - 24 is requested.

Trabelsi Fails to Teach All Claim Elements, Steps, and Limitations. In the Office Action dated May 4, 2005, authored by Examiner Abrishamkar, claims 1 - 24 were rejected under 35 U.S.C. §102(e) for lack of novelty as being anticipated by Trabelsi.

As specified in Claim 3 as originally filed, and as indicated as allowable in the first Office Action, a step, element or limitation of Appellants' invention which allows *reuse* of a finite number "action indicators" in association with a plurality of "action group tags" or "action group containers", wherein each action indicator combined with the group tag or container can be assigned a unique permission, was amended into the independent claims 1, 4, 9, 12, 17 and 20. In this manner, the number of permissions which can be controlled is expanded to beyond just the number of action indicators, but to an upper limit equal to the product of the number of allowable action indicators and the number of action tags or action containers.

By “action indicators”, Appellants mean the permission indicators for actions such as “attach”, “add”, “connect”, “delete”, etc., as discussed in paragraphs [0065] - [0066], Table 3, and paragraph [0071]. These are indicating allowable actions, not users. A user’s identity or identifier is contained elsewhere in the access control list, but is not the same as the action indicators.

By “action group container” and “action group tags”, Appellants mean a group of action indicators, not a group of users. Action indicators which are all related to each other for some

common reason or purpose, such as performing a system backup, can be grouped under a single action group tag, or contained in an action group container. These are not tags for groups of users, or containers for groups of users, as discussed in Appellants' paragraphs [0070] - [0078].

To extend the ability of defining permitted actions within the groups of actions, Appellants have disclosed and claimed the ability to "re-use" action indicators between multiple groups. For example, in systems without Appellants' invention, an action indicator of "r" might always permit a "read" action. But, with use of Appellants' invention, the action indicator "r" might permit a "read" action in an action group called "file_check_out", but the same action "r" might permit a "rewind" operation in an action group called "tape_operations", as discussed in Appellants' paragraphs [0070] - [0073].

As such, even with a fairly limited number of distinct action indicators, such as the 18 pre-defined action indicators of the embodiment which operates in cooperation with Tivoli's Policy Director, many more actions than 18 can be controlled based upon redefining each action indicator's meaning within multiple action group tags or multiple action group containers.

Regarding Trabelsi's Generic Groups of Permissions with Filters, Trabelsi is silent as teaching Appellants' action group containers and reusable action indicators. Trabelsi's "generic groups" of permissions are not containers of permissions, and Trabelsi's "filters" are not reusable action indicators, as Appellants have defined them and described them.

Trabelsi has disclosed that rights indicators or the resources themselves can be grouped into "generic groups" using "filters", where the filters can be a special character such as "*" or keywords such as "any" (emphasis added by Applicants):

> . . .
> [0043] The rights or the resources can be grouped into **generic groups** represented by **filters** in the form of **special characters** such as a star "*"or by **keywords** such as the word "any". The keyword "any" indicates, for example, any privilege. The table of FIG. 4 indicates exemplary meanings of the star filter. The "star" filter applied to a right with the format "xyz*" means any right whose name begins with xyz. The "star" filter applied to a resource type with the format "mytype*" means any resource whose type is mytype. The "star" filter applied to a resource path "/abc/def/*" means any resource whose path is a subpath of /abc/def/.
> [0044] **The filters and keywords make it possible to combine a large number of**

entries into one, and in this way to facilitate the management of the configuration.

. . .

Trabelsi's "filters" are functioning as wildcard characters according to this description. These filters act as wildcard operators in lists of permissions so that the traditional, single-meaning rights indicators can be easily incorporated into a larger group without actually specifying the indicator itself.

Consider Trabelsi's example group right called "xyz*". Trabelsi explains that this would include any right whose name begins with "xyz". So, for example, Applicants believe that this means the distinctively different rights "xyzopen" and "xyzdelete" in Trabelsi's way of naming rights (unlike Appellants' rights indicators which are individual characters), could be easily assigned to a user by giving that user a permission of "xyz*". This, however, does not mean that the filtered portions of the rights names, specifically "open" and "delete" in this example, could be *re-used* for some other meaning, as Appellants have claimed. For example, wouldn't "abcopen" and "abcclose" represent analogous rights to the resource "abc" compared to the rights "xyzopen" and "xyzclose" for the resource "xyz"? So, this same open+delete rights "group" could be specified by Trabelsi's invention as "abc*".

While this is useful, it is not the same as Appellants' claimed re-usable rights indicators, where a character, such as "k", can be used to indicate a right, such as "open", when it appears in a first rights container, but "k" can be re-used to indicate a different right, such as "delete", when it is used in a different rights container. Trabelsi's generic groups are not the same as containers of permissions, either.

To further corroborate Appellants' interpretation of Trabelsi's meaning of "filter" as a wildcard, note the French original disclosure available in Trabelsi's public PAIR Image File Wrapper. Especially note that the paragraphs corresponding to English translation paragraphs[0042] and [0043] utilize the French word "filtre" in place of the English word "filter":

9

Les droits ou les ressources sont susceptibles d'être regroupés en groupes génériques représentés par des filtres sous forme de caractères spéciaux tels qu'une étoile « * » ou par des mots-clés tels que le mot « any ». Le mot-clé « any » signifie par exemple tout privilège. Le tableau de la figure 4 indiquent des exemples de signification du filtre étoile *. Le filtre « étoile » appliqué à un droit de format « xyz* » signifie tout droit dont le nom commence par xyz. Le filtre « étoile » appliqué à un type de ressource de format « mytype* » signifie toute ressource dont le type est mytype. Le filtre « étoile » appliqué à un chemin de ressource « /abc/def/* » signifie toute ressource dont le chemin est un sous-ensemble de /abc/def/.

Les filtres et mot-clés permettent de regrouper un grand nombre d'entrées en une seule et de faciliter de ce fait l'administration de la configuration.

Trabelsi's Original Disclosure in French, Pg. 9, lines 1 - 13

According to a French-to-English information technology dictionary "Glossaire informatique des termes de la Commission ministérielle de terminologie informatique" (Glossary of Information Technology Terms from the Ministerial Commission for Terminology of Information Technology), available at http://www-rocq.inria.fr/qui/Philippe.Deschamp/CMTI/glossaire.html#F, Appellants find that "filtrage", which is the literal of English "filtering", is defined as:

Filtrage, n. m.

Voir : appariement de formes.

which refers the reader to the definition:

Appariement de formes, n. m.

Mise en correspondance de formes selon un ensemble prédéfini de règles ou de critères.

Synonyme : filtrage, n. m.

Anglais : pattern matching.

The English translation (Anglais) for French "filtre" is "pattern match". Pattern matching is synonymous with the function of wildcard characters such as "*" (e.g. anything starting with "abc" is found by pattern matching specification "abc*"). This, of course, is not referring to reusable characters in containers of characters, but instead is forming a super-group of permissions whose name or description match a pattern specification.

For these reasons, to interpret Trabelsi as disclosing Appellants' “action groups”, “action containers”, and Appellants' "reusable indicators" in the manner proposed in the rationale for the rejections would be improper importation of Appellants' definitions into the cited art. Appellants, therefore, requested in a previous reply to the examiner allowance of independent claims 1 - 24.

In response to the foregoing arguments, however, the Examiner has stated in the rationale for the final rejections that based upon the "broadest reasonable interpretation", each "action group tag" can be interpreted as the roles specified in Trabelsi's paragraph 0034. Specifically, the examiner has stated at page 2, line 18, of the Office Action, that Trabelsi discloses in paragraph 0043 the wildcard "effectively" "reuses" the permission indicators.

Regarding the word "re-use", this is injected into Trabelsi's disclosure by the examiner, and does not appear in paragraph 0043, or anywhere else in Trabelsi's disclosure. This is improper reading of the Appellants' disclosure into the cited art.

Regarding the "broadest reasonable interpretation in light of the specification", but the "specification is not read into the claims", this is an erroneous implementation of the relevant law and policy. The terms such as "permission indicator containers" and "action control lists" which appear in Appellants claims must be afforded the definitions and scope set forth in the Appellants' disclosure. This is not open to interpretation or broadening by the Examiner in light of art which would be useful to apply in a rejection.

In *Phillips v. AWH Corp.*, the Federal Circuit, sitting *en banc*, has clarified that the specification must be given priority over extrinsic sources of definitions, such as dictionaries, to affix scope and meaning to claim terms. *Phillips v. AWH Corp.*, 145 F. 3d 1303, 75 USPQ2d 1321 (Fed. Cir. 2005) (en banc).

Presumably, this priority of and reliance upon the specification, of which the claims as originally filed are an integral part, also trumps definitions which may be gleaned from cited art or from the examiner's own knowledge. This is only fair to applicants to allow them to use their

specification to describe their invention, and to conclude the specification with claims, where the claims are interpreted in light of the specification. Otherwise, it would be difficult if not impossible for applicants to develop claims in light of as-to-yet unknown art and unknown knowledge by an examiner who has yet to be assigned to examine the claims.

As such, the Examiner's refusal to afford meanings and scope to the Appellants' claim terms consistent with Appellants' disclosure, refusal to honor the previous holding of allowability by the first examiner of the case, and the failure of Tribelsi to teach all of the claimed elements, steps, and limitations represent errors in examination which must be corrected through the reversal of all rejections.

For these reasons, Appellants request allowance of Claims 1 - 24.

Respectfully Submitted,

Robert Frantz

Agent for Appellant(s)
Robert H. Frantz, Reg. No. 42,553
Tel: (405) 812-5613

Franklin Gray Patents, LLC
P.O. Box 23324
Oklahoma City, OK 73127
Tel: 405-812-5613
Fax: 405-440-2465

Claims Appendix

per 37 CFR §41.37(c)(1)(viii)

Clean Form of Amended Claims

Claim 1 (previously presented):

A method for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, said method comprising the steps of:

providing in a computer readable medium an access control policy associated with said requested protected system resource containing a permission list of permitted identities and at least one action group tag with associated action indicators;

reusing a finite quantity of action indicators among a plurality of action group tags to control a number of unique permissions less than or equal to the product of the quantity of allowable action indicators and a quantity of allowable action group tags;

evaluating said permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between permissible actions and members of a set of action indicators; and

granting to a requesting computer or program authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

Claim 2 (original):

The method as set forth in Claim 1 further comprising providing in an access control policy permission list a plurality of action group tags, each action group tag having one or more associated action indicators, such that resultant granting of authorization to act on said requested protected object is completed if the requested action is allowed by any of the associated action indicators of any of the action groups.

Claim 3 (previously presented):

The method as set forth in Claim 1 wherein said requested protected system resource comprises a computer file sent to a local computer from a remote computer over a computer network.

Claim 4 (previously presented):

A method for managing permission indicators for computer system protected objects comprising the steps of:

providing in a computer readable medium a plurality of permission indicator containers in an access control list;

associating a first set of permission indicators with a primary permission indicator container; and

associating in a computer readable medium accessible by an authorization control system one or more additional sets of permission indicators with additional permission indicator containers, wherein said permission indicators are reused among said containers such that permission indicators may be categorized and grouped logically to control a number of unique permissions less than or equal to the product of a quantity of allowable action indicators and a quantity of allowable action group tags.

Claim 5 (original):

The method as set forth in Claim 4 wherein said step of providing a first set of permission indicators comprises providing at least one other (additional) permission indicator set having equivalent permission indicators to said first set such that permission indicators may be assigned unique permissive control according to a permission indicator container with which they are associated.

Claim 6 (original):

The method as set forth in Claim 5 wherein said step of providing an equivalent set of permission indicators comprises providing the characters "a" through "z" and "A" through "Z" as permission indicators.

Claim 7 (previously presented):

The method as set forth in Claim 4 further comprising associating an action group tag with a permission indicator container.

Claim 8 (previously presented):

The method as set forth in Claim 7 further comprising the step of providing an action group tag with an associated list of permission indicators in an access control list entry.

Claim 9 (previously presented):

A computer readable medium encoded with software for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, said software performing steps comprising:

providing an access control policy associated with said requested protected system resource containing a permission list of permitted identities and at least one action group tag with associated action indicators;

reusing a finite quantity of action indicators among a plurality of action group tags to control a number of unique permissions less than or equal to the product of the quantity of allowable action indicators and a quantity of allowable action group tags;

evaluating said permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between members of a set of action indicators; and

granting authorization to perform actions on said requested protected system resource to said requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

Claim 10 (original):

The computer readable medium as set forth in Claim 9 further comprising software for providing in an access control policy permission list a plurality of action group tags, each

action group tag having one or more associated action indicators, such that resultant granting of authorization to act on said requested protected object is completed if the requested action is allowed by any of the associated action indicators of any of the action groups.

Claim 11 (previously presented):

The computer readable medium as set forth in Claim 9 wherein said requested protected system resource comprises a computer file sent to a local computer from a remote computer over a computer network.

Claim 12 (previously presented):

A computer readable medium encoded with software for managing permission indicators for computer system protected objects, said software performing steps comprising:

providing a plurality of permission indicator containers in an access control list;

associating a first set of permission indicators with a primary permission indicator container; and

associating one or more additional sets of permission indicators with additional permission indicator containers, wherein said permission indicators are reused among said containers such that permission indicators may be categorized and grouped logically to control a number of unique permissions less than or equal to the product of a quantity of allowable action indicators and a quantity of allowable action group tags.

Claim 13 (original):

The computer readable medium as set forth in Claim 12 wherein said software for providing a first set of permission indicators comprises software for providing permission indicators which are equivalent to at least one other (additional) permission indicators such that permission indicators may be assigned unique permissive control according to a permission indicator container with which they are associated.

Claim 14 (original):

The computer readable medium as set forth in Claim 13 wherein said software for providing equivalent permission indicators comprises software for providing a set of permission indicators including the characters "a" through "z" and "A" through "Z".

Claim 15 (previously presented):

The computer readable medium as set forth in Claim 12 further comprising software for associating an action group tag with a permission indicator container.

Claim 16 (previously presented):

The computer readable medium as set forth in Claim 15 further comprising software for providing an action group tag with an associated list of permission indicators in an access control list entry.

Claim 17 (previously presented):

An authorization system for extending and grouping actions and permissions for authorization of a requesting user to access or use a requested protected system resource in a computer system, said system comprising:

an access control policy disposed in a computer readable medium associated with said requested protected system resource, having a permission list of permitted identities and at least one action group tag with associated action indicators, wherein a finite quantity of action indicators are reused among a plurality of action group tags to control a number of unique permissions less than or equal to the product of the quantity of allowable action indicators and a quantity of allowable action group tags;

a permission list evaluator for evaluating an access control policy permission list according to a specific permission definition associated with said action group tag, said permission definition providing a correlation between members of a set of action indicators; and

an authorization grantor adapted to grant authorization to a requesting computer or program to perform actions on said requested protected system resource to said

requesting user if said access control policy permission list includes an appropriate action indicator correlated to an action group tag.

Claim 18 (previously presented):

The system as set forth in Claim 17 further wherein said access control policy permission list comprises a plurality of action group tags, each action group tag having one or more associated action indicators, such that resultant granting of authorization to act on said requested protected object is completed if the requested action is allowed by any of the associated action indicators of any of the action groups.

Claim 19 (previously presented):

The system as set forth in Claim 17 wherein said requested protected system resource comprises a computer file sent to a local computer from a remote computer over a computer network.

Claim 20 (previously presented):

A system for managing permission indicators for computer system protected objects comprising:

a plurality of permission indicator containers for an access control list, said access control list being disposed in a computer readable medium;

a first set of permission indicators associated with a primary permission indicator container; and

one or more additional sets of permission indicators associated in said computer readable medium with additional permission indicator containers, wherein said permission indicators are reused among said containers such that permission indicators are categorized and grouped logically to control a number of unique permissions less than or equal to the product of a quantity of allowable action indicators and a quantity of allowable action group tags.

Claim 21 (previously presented):

The system as set forth in Claim 20 wherein said first set of permission indicators and at

least one other (additional) permission indicator set are equivalent permission indicators such that permission indicators are assigned unique permissive control according to the permission indicator container with which they are associated.

Claim 22 (original):

The system as set forth in Claim 21 wherein said equivalent set of permission indicators comprises the characters "a" through "z" and "A" through "Z".

Claim 23 (original):

The system as set forth in Claim 20 further comprising an action group tag associated with a permission indicator container.

Claim 24 (previously presented):

The system as set forth in Claim 23 further comprising an action group tag associated with a list of permission indicators in an access control list entry.

Evidence Appendix

per 37 CFR §41.37(c)(1)(ix)

No evidence has been submitted by applicant or examiner pursuant to 37 CFR §§1.130, 1.131, or 1.132.

Related Proceedings Appendix

per 37 CFR §41.37(c)(1)(x)

No decisions have been rendered by a court or the Board in the related proceedings as identified under 37 CFR §41.37(c)(1)(ii).